**PortSwigger Access Control Vulnerability**

**Intern id:** 195

**Lab :** Unprotected admin functionality with unpredictable URL

**Environment :** Linux

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Objective**

Demonstrate that the application exposes an administrative function at a non-obvious URL, but without proper authentication or authorization checks. By discovering the hidden endpoint, an attacker can perform privileged actions.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Target**

Application: PortSwigger Access Control Lab – Admin with Unpredictable URL

Vector: Hidden /administrator-panel endpoint

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Vulnerability Description**

The application does not properly enforce access control on the admin panel. While the link to the panel is not directly visible in the UI, it is still accessible if an attacker discovers its location (e.g., through JavaScript files, comments, or forced browsing).

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Steps to Reproduce**

1. Log in as a normal user (e.g., wiener:peter).

No admin links are visible.

2. Inspect the site for clues:

Open Developer Tools → Sources.

Check JavaScript files (e.g., /static/js/app.js).

In one file, find a reference to:

/admin-abc123

(an “unpredictable” URL for the admin panel).

3. Manually request the hidden admin panel:

https://<lab-url>/admin-abc123

→ The page loads without requiring admin privileges.

4. Perform an administrative action:

https://<lab-url>/admin-abc123/delete?username=carlos

→ The request succeeds, deleting user carlos.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Technical Explanation**

The backend should enforce authorization checks like:

GET /admin-abc123/delete?username=carlos

Cookie: session=attacker

But instead, it processes the request without validating the requester’s role.

The unpredictability of the URL is security through obscurity, which is insufficient.

Once the URL is discovered, attackers gain full admin access.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Impact**

Attacker can discover hidden admin endpoints.

Enables privilege escalation and account deletion.

Security depends only on the secrecy of the URL, not on proper access control.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Mitigation**

Enforce role-based access control (RBAC) on all admin functions.

Never rely on “unpredictable” or “hidden” URLs for security.

Require strong authentication & authorization for privileged pages.

Regularly scan code and assets for exposed sensitive paths.

**\_\_\_\_\_\_\_\_\_\_\_ THANK YOU \_\_\_\_\_\_\_\_\_\_\_**